#2

E4921-01

INFORMATION UNDER 37 CFR 1.56(a)

(For Initial Filing)

The following references are submitted as information to comply with the duty of disclosure under 37 CFR 1.56(a):

References	Disclosed in the specification?		Copy			Translation	
	Yes	No	Enc.	Follow	Please obtain	Enc.	Not available
1. D.V.Chudnovsky, G.V.Chudnovsky "Sequences of Numbers Generated by Addition in Formal Groups and New Primality and Factorization Tests", Advances in Applied Mathematics, 7, 385-434, 1986	×		×				
2. P.Montgomery, "Speeding the Pollard and Elliptic Curve Methods of Factorization", Mathematics of computation Vol.48, No.177, pp.243-264(1987)	×		×				
3. IEEE P1363/D2 Standard Specification for Public Key Cryptography (1998)	×		×				
4. Henri Cohen, "A Course in Computational Algebraic Number Theory", GTM138, Springer(1993) p.464 Atkin's Test	×		×				
5. A.Menezes, P.Oorschot, S.Vanstone, "Handbook of Applied Cryptography", CRC Press(1996) Section 4.5.3 Primitive polynomials	×		×				

12 December 2003